REMARKS

Claims 1-36 are pending in this application. Applicant thanks the Examiner for the interview on November 30, 2006. Reconsideration of the pending claims is respectfully requested.

Claims 1-36 have been rejected under 35 U.S.C. §102(b) as being anticipated by Rothermel et al. (US 6,678,827). Claim 1 recites a method comprising *creating* a plurality of templates, and *expanding* at least one template at a central location. The limitation of expanding at least one template at a central location is not taught by Rothermel et al. The Examiner initially pointed to col. 5 lines 1-10 of Rothermel et al. for this limitation (Office Action 1/30/06 page 2). Applicant rebutted in an Amendment received in the Patent Office on May 30, 2006. The Examiner next pointed to col. 10 line 8 to col. 11 line 17 (Final Office Action 8/23/06 page 2).

As discussed with the Examiner in the recent interview, the newly referenced portion of Rothermel et al. notes that "FIGS. 3C-3H provide exemplary graphical user interface screens such as may be provided by a manager device to assist in *defining security policy templates*. Referring now to FIG. 3C, a variety of aliases are available to be used in *creating security policy templates*." (col. 10 line 66 to col. 11 line 3, emphasis added). Here, Rothermel et al. teaches that the manager device can *define* or *create* templates, but not that these templates are being expanded at a central location, as required by claim 1.

Moreover, taken as a whole, Rothermel et al. is quite clearly teaches creating templates at a central location and expanding the templates at decentralized locations, namely, at the multiple network security devices (NSDs). For example, the Abstract states that "[t]he system allows the manager device to create a consistent security policy for the multiple NSDs by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information." The Summary (col. 3 lines 31-35), and the Detailed Description (col. 4 lines 32-38) recite essentially the same methodology of distributing a template for remote configuration.

Those portions of the Detailed Description of Rothermel et al. that discuss configuring the security policy template do not teach or suggest anything other than configuration by the NSDs and clearly does not teach configuration by the manager device. As an example, "FIG. 3B shows that the security policy template 300 contains a number of security policy filter rules,

including security policy rule 301." (col. 10 lines 27-29). "When the security policy template 300 and the network profile 310 for network 1 are combined to create the security policy 315 for network 1, the facility replaces the "InformationServices" alias in rule 301 with the network addresses listed for the "InformationServices" alias in definition 311. Doing so produces rule 316 in the security to policy 315 for network 1" (col. 10 lines 47-53). Here, neither FIG. 3B, nor the supporting specification, indicates whether the configuration is performed by network 1 or by the manager device. The specification merely notes that "the facility" replaces the alias with the network addresses. However, there is certainly nothing in FIG. 3B or the supporting specification to suggest that the manager device constitutes "the facility," whereas Applicant has shown three clear statements from the Abstract, Summary, and Detailed Description that explicitly state that it is the NSDs that configure copies of the template with NSD-specific information.

As another example, Rothermel et al. provides:

> In order to remotely manage multiple NSDs, a manager device can use one or more intermediate supervisor devices. For example, after a security policy template is defined, the manager device can distribute the template to multiple NSDs by sending a single copy of the template to a supervisor device associated with the NSDs and by then having the supervisor device update each of the NSDs with a copy of the template. Each of the NSD template copies can then be configured with NSD-specific information from one or more of a variety of sources, such as by the manager device, by a local user such as a system administrator, or automatically such as with DNS information. (col. 4 line 63 – col. 5 line7)

Here, the manager device distributes a defined security policy template to an intermediate supervisor device which then updates each of the NSDs with a copy of the template. Each of the NSD template copies can then be configured with NSD-specific information. Although there is an intermediate supervisor device between the manager device that defines the template and the NSDs that configure the template copies with NSD-specific information, there is no suggestion that anything other than the NSDs perform the actual configuration. It is noted that the NSD-specific information can be supplied to the NSDs by a variety of sources, such as by the manager device, but this does not teach or suggest that the manager device actually configures template copies with NSD-specific information prior to distributing the template to the intermediate supervisor devices. Such a reading would also be inconsistent with the notion of "sending a single copy of the template to a supervisor device" for further distribution to multiple NSDs. In

such a situation, if the single copy were configured with NSD-specific information for one network, the copy would not be appropriately configured for the other networks.

Accordingly, Applicants have shown that Rothermel et al. does not teach the limitation of expanding at least one template at a central location. Rothermel et al. is clear that configuration of the NSDs takes place at the NSDs, even when the manager device supplies both the template and the NSD-specific information to the NSD. Thus, claim 1, and claims 2-7 depending therefrom, are novel over Rothermel et al.

Applicant notes that independent claim 8 similarly recites a system comprising a plurality of agents in communication with a communications gateway configured to expand templates and provide the expanded information to the agents. If the manager device of Rothermel et al. reads on the communications gateway of claim 8, it will be clear from the discussion above that the manager device does not expand templates, as required by claim 8. Thus, claim 8, and claims 9-21 depending therefrom, are novel over Rothermel et al.

Independent claim 22 similarly recites a method comprising retrieving a template and creating a document comprising a listing of users identified by any externally referenced information, and providing the document to a device. In Rothermel et al., although each NSD retrieves a template and creates a document from externally referenced information, these documents are not thereafter provided to other devices. Thus, claim 22, and claims 23-30 depending therefrom, are novel over Rothermel et al. Independent claim 31 similarly recites a method comprising retrieving a template, creating a document, and providing the document to a device. As noted, documents created from templates by the NSDs in Rothermel et al. are not further distributed. Thus, claim 31, and claims 32-36 depending therefrom, are novel over Rothermel et al.

In view of the above, Applicants requests that the Examiner withdraw the rejections of claims 1-36 under 35 U.S.C. §102(b).

Applicant also discussed with the Examiner on November 30, 2006 certain dependent claims that were further patentable over Rothermel et al. In particular, Applicant pointed to claim 15 which recites that the document is an XML document. Applicant noted that the limitation is not expressly recited by Rothermel et al. The Examiner suggested that an address in HTTP read on the limitation of an XML document. In the interview, Applicant distinguished

XML from HTTP. Applicant pointed out that XML (eXtensible Markup Language) is a language that allows for the creation of customized tags when creating documents that offer flexibility in organizing and presenting information. In contrast, HTTP (Hypertext Transfer Protocol) is a protocol used to carry requests from a browser to a Web server and to transport pages from the Web server back to the requesting browser. Since XML is a language and not a protocol, an address in HTTP does not read on the limitation of an XML document. Applicant contends that claims 15, 23 and 32, which recite an XML document, are allowable over Rothermel et al.

Applicant also sought to rebut the Examiner's contention on page 7 of the Office Action dated January 30, 2006, that claims 22-36 "are directed to the same method as found in claims 1-21 in slightly reworded form." Applicant particularly cited to claims 28 and 29 as examples of claims that recited limitations that are not slightly reworded variants of previously examined claims. Claim 28, for instance, recites that "a template in said second category inherits policies contained in a template of said first category." Applicant pointed out that Rothermel et al. does not discuss inheritance and that the limitation has no analog in the prior claims. Likewise, claim 29 adds to claim 28 the further limitation that "the inheritance can be selectively disabled." Here, too, selective disablement has no analog in the prior claims. Accordingly, Applicant contends that claims 22-36 have not been properly examined and that at least claims 28 and 29 are further patentable over Rothermel et al.

All pending claims are now allowable and Applicant therefore respectfully requests a Notice of Allowance from the Examiner. Should the Examiner have questions, the Applicant's undersigned agent may be reached at the number provided.

Respectfully submitted,

Gordon Good

Date: January 23, 2007 By: Daniel C. Kloke

Daniel C. Kloke, Reg. No. 58,417
Carr & Ferrell *LLP*
2200 Geng Road
Palo Alto, CA 94303
TEL: (650) 812-3465
FAX: (650) 812-3444